Docket No. PF02025NA/10-29

METHOD AND APPARATUS FOR PROVIDING NODE SECURITY IN A ROUTER OF A PACKET NETWORK

FIELD OF THE INVENTION

This invention relates in general to data communication systems, and more specifically to a method and apparatus for providing node security in a router of a packet data network.

BACKGROUND OF THE INVENTION

Packet data communication networks that are accessible to the public are subject to intrusion and disruption by predatory elements, such as hackers. By targeting a few critical nodes with a destructive virus or worm, it is possible to take down an entire network. Prior-art routers have done little more than reading header information and forwarding each data packet to the destination indicated in the associated header. This has provided no protection to destination devices, including computers and other routers that might be harmed by the user data carried by the data packet.

Thus, what is needed is a method and apparatus for providing node security in a router of a packet network. Preferably, the method and apparatus will be able to detect and eliminate potentially harmful data packets soon after they enter the network, and before they can reach destinations where they can produce widespread harm.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an electrical block diagram of an exemplary packet data communication network in accordance with the present invention.

FIG. 2 is an electrical block diagram of an exemplary router in accordance with the present invention.

FIG. 3 is a flow chart depicting operation of the exemplary router in accordance with the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Referring to FIG. 1, an electrical block diagram 100 of an exemplary packet data communication network in accordance with the present invention comprises an originator 102 that transmits data packets through the network. The originator can employ, for example, a workstation, a personal computer, or a portable or wireless multimedia device to transmit the data packets. The network can comprise an entry router 104 and various combinations of wired or wireless local area networks (LAN) 106, intermediate routers 108, 110, 112, a wide area network (WAN) 114, and one or more servers 116. A typical destination of the data packets is, for example, the server 116. When the originator has malicious intent and wishes to harm all or part of the network, the destination can be either the server 116 or one or more of the routers 104, 108, 110, 112.

One aspect of the present invention is to involve the routers of the network more effectively than has been done in the prior art, in order to detect and intercept harmful data packets, such as viruses, worms, and Trojan horses at the earliest possible point after entry into the network and before much of the network can become infected. Another and related aspect provides a "healing" methodology for the network or components within the network. For example, when the originator 102 is attempting to send harmful data packets into the network, the entry router 104 is the preferred choice for blocking the harmful data packets. In one embodiment, one or more of the downstream routers, e.g., the router 112, can be designated an "enhanced security" router, in that it can be programmed with more sophisticated detection mechanisms for locating harmful data packets than the upstream routers, and it would then collaborate with the upstream routers to coordinate and control the efforts to eradicate the

harmful data packets thus facilitating the above mentioned healing effect. This would allow some economic trade-offs to be made. Various techniques will be described further herein below for providing the collaboration among the routers of the network in accordance with the present invention to successfully detect and intercept harmful data packets near and over time even nearer their entry point.

Referring to FIG. 2, an electrical block diagram of an exemplary router 200 in accordance with the present invention comprises a plurality of input/output (I/O) ports (1-N) 202 for communicating with other nodes of a network. More specifically, the I/O ports are for accepting a data packet sent from an originator via the router 200 and addressed to a destination device other than the router 200, and for transmitting the data packet to the destination device. The I/O ports 202 are coupled to a processor 208 for processing the data packet in accordance with the present invention.

The processor 208 preferably comprises a memory 210 containing software and operating parameters for programming the processor 208. The memory 210 comprises a routing control program and database 212 for controlling the routing of data packets through well-known techniques. It will be appreciated that, for additional speed, the router 200 also can comprise special purpose hardware for routing the bulk of the data packets. The memory 210 also includes a node security program 214 for programming the processor 208 in accordance with the present invention. The node security program 214 programs the processor 208 to monitor selected data packets as they enter the router 200, and to determine, on the fly or in near realtime, whether the data packets are potentially harmful to the destination device (or, alternatively, to the router 200 itself). The monitoring preferably begins with scrutinizing the nature of the control headers of the data packets for corruption.

Depending on the traffic the router 200 is handling, as well as a history of recently encountered harmful data packets, the monitoring can be done in several different manners. These include: random sampling of a subset of data packets; monitoring data packets having a predetermined source address; monitoring data packets having a predetermined destination address; or monitoring data packets having a predetermined combination of source and destination address. It will be appreciated that selection of the data packets to be monitored can also take into account the port numbers used by the source or the destination. Advantageously, random sampling of data packets reduces the processing burden on the router, and the sampling rate can be adjusted according to traffic and the frequency of attacks. Address-specific monitoring advantageously allows focusing on known suspicious originators and/or targeted destinations.

The node security program 214 further programs the processor 208 to interrupt transmission of the data packet in response to determining that the data packet is potentially harmful to the destination device, including communicating with a second router to cause the second router to interrupt transmission of a future data packet; and to transmit the data packet in response to determining that the data packet is not potentially harmful to the destination device. Once the decision has been made to interrupt the transmission of the data packet, the processor 208 can also be programmed to interrupt or discard later sent data packets from the same originator.

There are several techniques that the node security program 214 uses to detect harmful data packets. One known technique is to check for signatures or data patterns that can indicate the potential presence of known viruses, worms, Trojan horses, and the like. Also, because a definitive determination often is impossible after examining only a single data packet, when the processor 208 determines that a

first data packet is suspicious, e.g., the data packet resembles something harmful but additional data packets are required to confirm, the processor 208 preferably decides to monitor future data packets having at least one of the source address and the destination address of the first data packet, until a definitive determination can be made. In addition, the processor 208 preferably examines the headers of data packets, looking for corruption and/or the presence of executable code as is known, particularly when such corruption and/or code originates from a single source. In addition, user data in the data packets can be analyzed by known methods to determine whether it contains executable code. Diagnostic software also can be executed to check whether doubtful or sample-picked hardware or software in the network have been tampered with.

The memory 210 also includes an up/downstream collaboration program 216 for programming the processor 208 to collaborate with other routers to block harmful data packets. The processor can, for example, send, using known techniques, a command addressed to the originator of harmful data, requesting address information for the routers participating in the handling of the command. Examples are the IP Ping and IP Traceroute commands. From the response, the processor 208 can learn the address of at least one upstream router that could have been used by the originator as the entry point to the network. The processor 208 then preferably collaborates with the at least one upstream router to intercept transmissions of the originator. This can be accomplished through a variety of techniques. For example, the processor 208 can send a command to the upstream router to intercept future data packets from the originator. Alternatively, the processor 208 can forward an agent (e.g., the agent 220) to the upstream router, where the agent is arranged to intercept a future data packet from the originator, through known techniques. Another option

is for the processor to cause the upstream router to update its capabilities (e.g., virus database) to detect a potentially harmful data packet. It should also be appreciated that the upstream router need not be a neighbor of the requesting router in order to have the upstream router block transmissions from the originator. That is, the upstream router can be remotely connected to the requesting router through other routers, LANs, and WANs.

In addition, the memory 210 includes a learning program 218 for programming the processor 208 to learn about, through known techniques, e.g., from adulterated headers and suspicious user data, new harmful signatures to screen for. The new harmful signatures preferably are then communicated to upstream collaborating routers in the network. This advantageously can result in a dynamic, iterative, detect/warn/contain process for intercepting harmful data packets that provides a network healing effect. It is thus to be understood that the method and apparatus in accordance with the present invention advantageously provides a simple and effective way to intercept harmful data packets at or very near their entry point into the network.

Referring to FIG. 3, a flow chart 300 depicts operation of the exemplary router 200 in accordance with the present invention. Flow begins with the router 200 monitoring 302 a selected data packet as described above. The router 200 then determines 304 whether the data packet is harmful, using at least one of the techniques outlined above. If so, the router 200 interrupts 306 the transmission of the data packet, and communicates 307 with at least a second router to cause the second router to interrupt a future data packet, as disclosed herein above. If, on the other hand, at step 304 the router 200 determines that the data packet is not harmful, the router 200 then transmits 308 the data packet towards the intended destination.

It should be clear from the preceding disclosure that the present invention makes available a method and apparatus for providing node security in a router of a packet network. Advantageously, the method and apparatus is able to detect and eliminate potentially harmful data packets soon after they enter the network, and before they can reach destinations where they can produce widespread harm. This provides the healing effect for the network in the event harmful data is allowed to enter.

Many modifications and variations of the present invention are possible in light of the above teachings. Thus, it is to be understood that, within the scope of the appended claims, the invention can be practiced other than as described herein above.